ALPHAVILLE

Part of the Someone is wrong on the internet series

FUD, inglorious FUD

44

APRIL 24, 2018 11:00 PM
By: **Jemima Kelly**

Read more articles in **SOMEONE IS WRONG ON THE INTERNET SERIES**

IOTA, an internet-of-things-focused cryptocurrency designed to allow machines to send data and micropayments between each other, has the backing of some big industrial companies and a $6bn (https://coinmarketcap.com/) valuation - more than Slack, the SoftBank-backed workplace messaging app with 6 million users (https://www.statista.com/statistics/652779/worldwide-slack-users-total-vs-paid/).

It also has a buzzy investor following. Veteran Wall Street analyst and hedge fund manager, James Waggoner, wrote a post (https://hacked.com/why-iota-belongs-on-your-focus-list/) on Hacked.com last week explaining why it should be on investors' “focus lists”. It's a “techno triple play” on three of the biggest trends going, he enthused: cryptocurrencies, the internet of things, and artificial intelligence.

Yet IOTA also highlights something else, a factor not unique to the crypto boom but one which highlights the tensions between tech utopianism and the big money at stake. An open and collaborative approach to developing standards, software and security protocols can be hard to sustain in a gold rush.

A tangled web

IOTA is one of a new wave of cryptocurrencies that aren't actually underpinned by a blockchain. (We'll explore the rise of postblockchainism in future posts.)

Instead, it is underpinned by what techy types call a “ directed acyclic graph (https://en.wikipedia.org/wiki/Directed_acyclic_graph)” or DAG, which IOTA calls the “tangle”. It says the tangle can solve the problems of scalability and high transaction fees (https://bitinfoch arts.com/comparison/bitcoin-transactionfees.html) suffered by bitcoin and other cryptos because rather than using a network of miners to process transactions, they are processed by those involved in the transactions.

Here's an illustration of the tangle, from IOTA's white paper (https://assets.ctfassets.net/r1dr6vzfxhev/4i3OM9JTleiE8M6Y04Ii28/d58bc5bb71cebe4adc18fadea1a79037/Tangle_White_Paper_v1.4.2.pdf):

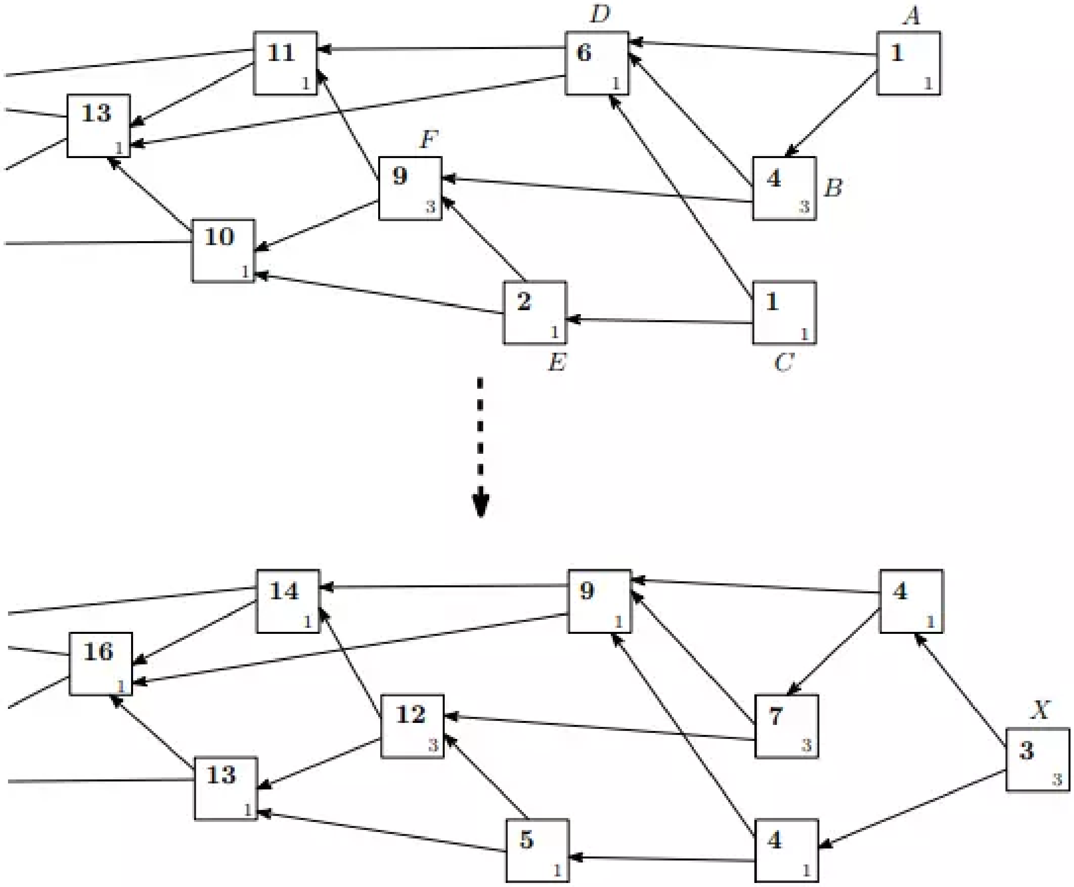


Figure 1: DAG with weight assignments before and after a newly issued transaction, X. The boxes represent transactions, the small number in the SE corner of each box denotes own weight, and the bold number denotes the cumulative weight.

The promise of a decentralised cryptocurrency that can enable machines to send data and micropayments to each other has pulled in a lot of hype (https://oracletimes.com/this-is-why-you-should-invest-in-iota-miota-immediately/) and investment, including from Bosch. The 132-year-old German engineering and electronics firm in December became the first major company to buy crypto tokens, via Robert Bosch Venture Capital, which it said had bought a " significant amount (http://www.bosch-presse.de/pressportal/de/en/robert-bosch-venture-capital-makes-first-investment-in-distributed-ledger-technology-137411.html)" of IOTA.

Security is numero uno

But it turns out that IOTA, for the time being anyway, is not decentralised (remind you of anything (https://ftalphaville.ft.com/2018/01/05/2197220/the-ripple-effect/)?). IOTA says that's because it's in a “transition period”, and that until it become deployed on a large scale, it needs a “Coordinator” to protect against attacks on the IOTA network.

If it's not decentralised, and therefore not censorship-resistant (https://medium.com/pandoraboxchain/censorship-resistance-and-public-blockchains-7e1dd41537d5), IOTA's USP becomes a little less clear (https://medium.com/@ercwl/hello-david-b77bbc62c457). To quote one developer who wanted to stay anonymous,

> If I don't have to build a decentralized system, I can build much faster, better schemes than IOTA. It's like a plane that travels on land. You really shouldn't design it with wings. It only goes on land. A car body would be far better in every conceivable way.

IOTA founder David Sonstebo told us the following:

> IOTA itself is decentralised, however, due to the fact that it's built for real-life applications in large-scale deployments it needs to reach a critical mass before it's 100% safe against attacks, therefore there is a Coordination node that you can voluntarily follow instructions from for security purposes. The people that think this is a problem simply know nothing about development. It is safety wheels, would you put a toddler on a bike without a helmet and kneepads? Hopefully not, likewise with cutting-edge tech. For us security is numero uno, and we didn't create IOTA for some opaque fringe ideological reason, we made it for the real world, thus we follow the sane and iterative development and deployment.

OK, so security is numero uno for IOTA. That makes sense.

Thing is, a whole (https://twitter.com/peterktodd/status/938397135862714373?lang=en) lot (https://github.com/iotaledger/wallet/issues/734) of people (https://www.forbes.com/sites/jeffkauflin/2018/01/03/iota-rose-464-in-2017-but-buyer-beware-experts-have-major-security-concerns/#6c0c9d115faa) don't think much of IOTA's security, either.

In September, a group of researchers from MIT's Digital Currency Initiative (https://dci.mit.edu/) (DCI) published a post (https://medium.com/@neha/cryptographic-vulnerabilities-in-iota-9a6a9ddc4367) on online platform Medium saying they had found a “cryptographic vulnerability” in IOTA's hash function, which IOTA calls “Curl”, which had enabled them to forge signatures on IOTA payments.

(The hash function (https://en.wikipedia.org/wiki/Hash_function) is a mathematical process that all cryptocurrencies rely on, which takes a bunch of data of any size and spits out output data of a fixed size - the so-called hash. The one bitcoin uses (https://en.bitcoin.it/wiki/SHA-256) was designed by the U.S. Government - the NSA to be precise - and hash functions are generally considered very difficult to get right, so the researchers had suspected IOTA's hash function might not be bulletproof before undertaking their research.)

Such forgery, the team said, could be used by a bad actor to steal funds.

IOTA, which has since fixed the flaw, denies that, saying the Coordinator would have prevented the forgery. (Turns out centralised authorities (https://www.federalreserve.gov/) are quite effective for security!) It says (https://blog.iota.org/official-iota-foundation-response-to-the-digital-currency-initiative-at-the-mit-media-lab-part-2-9ce650ad789c) there's a conflict of interest in the research because of the work of one of the lead researchers, Ethan Heilman, on other DAG protocols (https://www.daglabs.com/), and the DCI's association with bitcoin core developers (https://medium.com/mit-media-lab-digital-currency-initiative/announcing-a-900-000-bitcoin-developer-fund-6e8b7e8b0861).

But it also says it wrote the flaw into the code deliberately, to protect investors. Some might think that sounds a bit far-fetched (https://www.reddit.com/r/ethereum/comments/6ywd9x/iota_team_claims_that_they_intentionally_broke/); others - including Ethereum's prodigy creator Vitalik Buterin (https://www.ft.com/content/b09d004e-4197-11e8-803a-295c97e6fd0b) - think (https://www.reddit.com/r/Iota/comments/720rg2/vitalik_buterins_response_to_iota_criticism/) writing malicious code into open-source protocols goes against the open-source spirit somewhat.

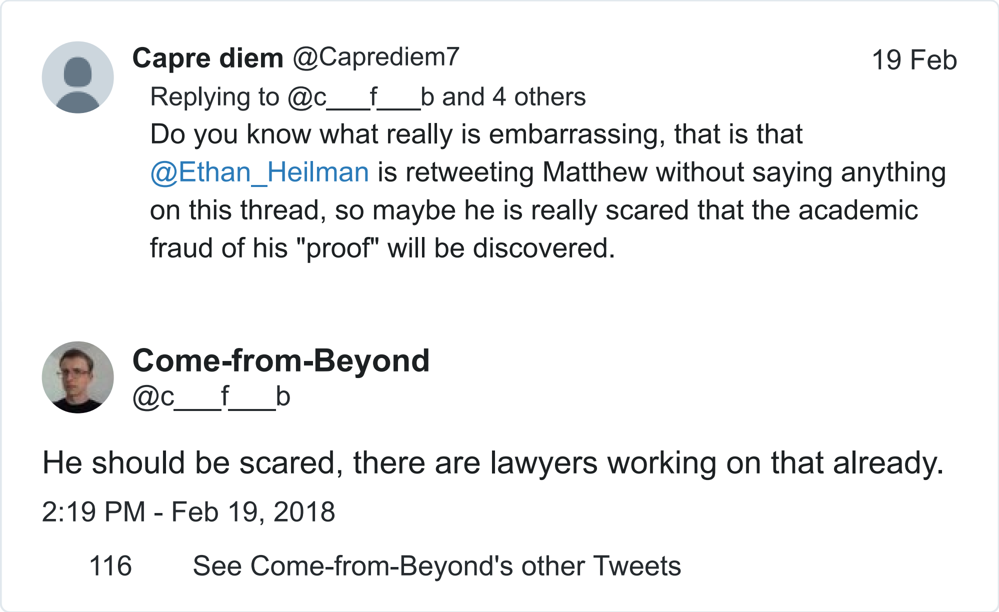
Here's how Sonstebo put it to us:

> This is an environment where a lot of scammers copypaste code and create nonsense ICOs that effectively lead to the loss of hundreds of millions of dollars for people, keeping this in mind we decided that we'd do what we could to prevent anyone from exploiting IOTA to exploit others, thus temporary copy protection.

Thin skin in the game

IOTA talks a lot about FUD (fear, uncertainty and doubt), a term adopted by the crypto community to refer to critical commentary. The acronym might also reasonably be applied to its own approach to dealing with critics.

For instance, here's Sergei Ivancheglo, an IOTA founder who uses the Twitter handle Come-from-Beyond, on Mr Heilman's work:



Capre diem @Caprediem7 19 Feb

Replying to @c___f___b and 4 others

Do you know what really is embarrassing, that is that @Ethan_Heilman is retweeting Matthew without saying anything on this thread, so maybe he is really scared that the academic fraud of his "proof" will be discovered.

Come-from-Beyond
@c___f___b

He should be scared, there are lawyers working on that already.

2:19 PM - Feb 19, 2018

116 See Come-from-Beyond's other Tweets

Asked about the tweet, Mr Sonstebo said neither he or the IOTA Foundation has ever threatened any legal action against researchers. He said for Mr Ivancheglo it was a matter of reputation, and “ Sergey felt he had no choice but to seek legal counsel. This never had anything to do with IOTA, it was a personal dispute between two people.”

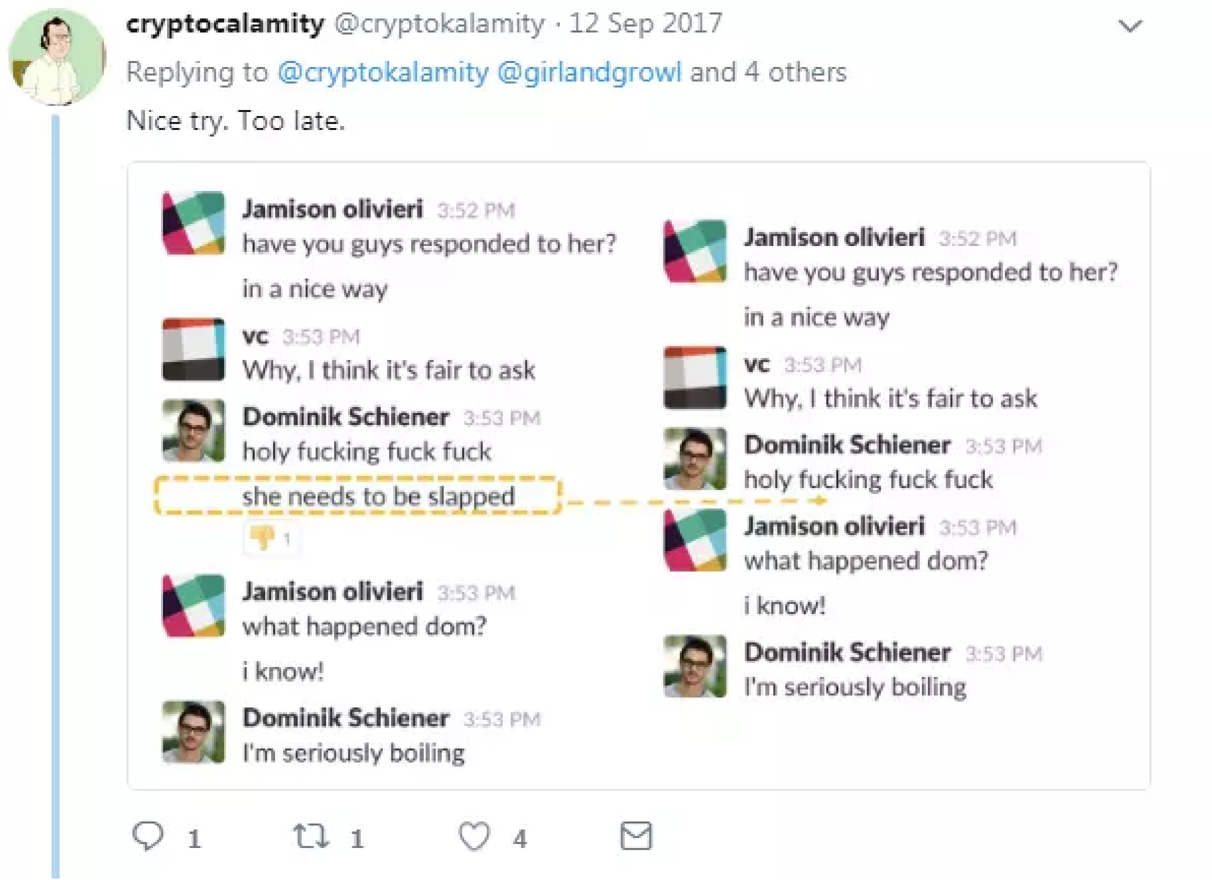
Mr Sonstebo also said IOTA had been “the target of a smear campaign” and that a series of leaked emails (http://www.tangleblog.com/wp-content/uploads/2018/02/letters.pdf) between the DCI researchers and IOTA corroborated their side of the story.

One of those, email #76, was from Mr Sonstebo to Neha Nerula, the author of the Medium post and one of the DCI researchers. It said:

> We will use all resources to elucidate this as publicly as possible if Ethan does not effective immediately contact all the people he has been spreading this premature story to and retract all his statements.

Mr Sonstebo didn't respond to a question on what “all resources” meant.

When Amy Castor, a freelance contributor to Forbes, wrote this piece (https://www.forbes.com/sites/amycastor/2017/09/07/mit-and-bu-researchers-uncover-critical-security-fla w-in-2b-cryptocurrency-iota/#7b5ab9e97570) on the MIT findings, the reaction inside IOTA was not a happy one, according to this guy on Twitter (https://twitter.com/cryptokalamity). He posted what appears to be a screenshot of an edited Slack conversation featuring Dominik Schiener, another IOTA co-founder:

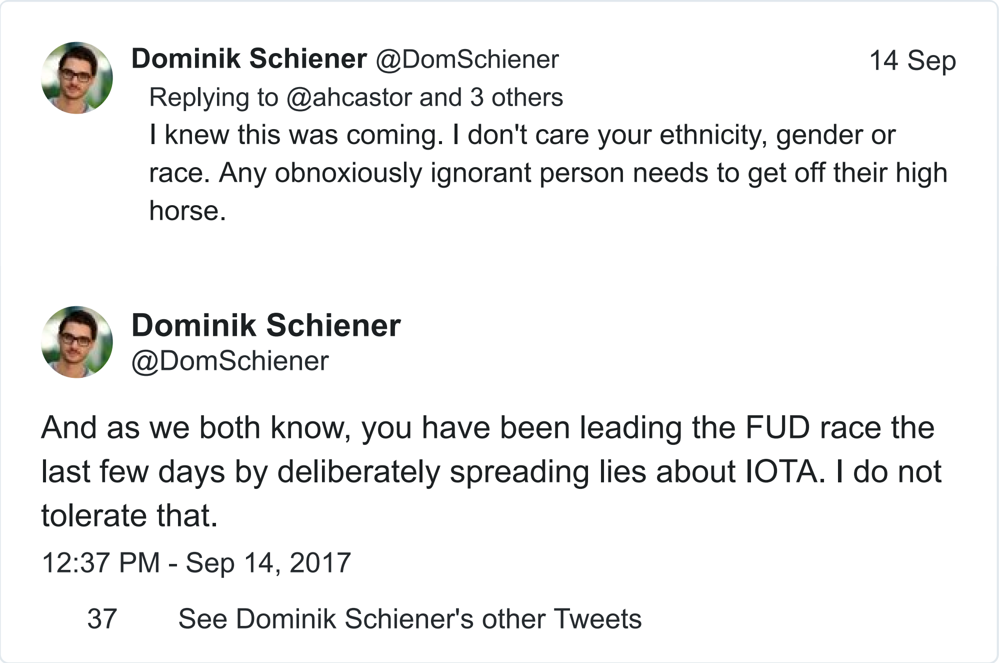


cryptocalamity @cryptokalamity · 12 Sep 2017
Replying to @cryptokalamity @girlandgrowl and 4 others
Nice try. Too late.

Jamison olivieri 3:52 PM
have you guys responded to her?
in a nice way
vc 3:53 PM
Why, I think it's fair to ask
Dominik Schiener 3:53 PM
holy fucking fuck fuck
she needs to be slapped
👎 1
Jamison olivieri 3:53 PM
what happened dom?
i know!
Dominik Schiener 3:53 PM
I'm seriously boiling

Jamison olivieri 3:52 PM
have you guys responded to her?
in a nice way
vc 3:53 PM
Why, I think it's fair to ask
Dominik Schiener 3:53 PM
holy fucking fuck fuck
Jamison olivieri 3:53 PM
what happened dom?
i know!
Dominik Schiener 3:53 PM
I'm seriously boiling

Mr Schiener responded to the original unedited version, which was then shared by Castor (https://twitter.com/ahcastor/status/908380975721304064), with the following:



Dominik Schiener @DomSchiener 14 Sep
Replying to @ahcastor and 3 others
I knew this was coming. I don't care your ethnicity, gender or race. Any obnoxiously ignorant person needs to get off their high horse.

Dominik Schiener
@DomSchiener

And as we both know, you have been leading the FUD race the last few days by deliberately spreading lies about IOTA. I do not tolerate that.
12:37 PM - Sep 14, 2017

37 See Dominik Schiener's other Tweets

There is also swearing at other journalists (https://twitter.com/davidsonstebo/status/966445336364486656?lang=en) on Twitter, and " blacklisting (https://twitter.com/iotatoken/status/966309603389698048?lang=en)" news sites that publish critical articles.

IOTA's "troll army" - which is how its team of online disciples is often (https://twitter.com/ShitcoinDotCom/status/963828911602716673) referred (https://twitter.com/matthew_d_green/status/965587523513864192) to as - have scared off some people enough for them not to want to speak out. Two people we asked to speak to for this story told us they didn't want to because they were worried about the consequences of doing so. One was worried about being threatened with physical harm.

Tim Swanson, founder of tech consultancy Post Oak Labs and a leading authority in the space, told us he undid a retweet of a story that was mildly critical of IOTA because he felt intimidated by Skype messages from a senior person from the IOTA team that were sent after sharing the article.*

Swanson is concerned that these kinds of incidents could provide a chilling effect, discouraging other researchers from doing the important work of testing the network before investors put their money into it:

> Ignoring for the moment any of the technical problems that independent researchers may have highlighted about the cryptography or the platform itself, it's the reaction to any kind of critical feedback that is a concern.
>
> Once you start threatening independent research teams that do vetting and verification...you're not just creating ill will, but you're actually creating an environment in which security researchers no longer feel safe to provide independent verification of claims which benefit society as a whole.
>
> If the ethos of the distributed ledger world is to be open and transparent, and to be inclusive of different ideas... then suing people because they think they found some problem just seems like the antithesis of what this is about. I'm not all about the philosophy of distributed ledger technology; I just think this is ironic.

Did we mention this project is apparently valued at $6bn?

**Update: we have edited this to show it was Skype messages, not an email, that were sent to Mr Swanson.*

Related links:

Sell all crypto and abandon all blockchain (https://www.ft.com/content/43ae0e68-857e-3f0e-af53-6ea78b9fd13c) - FT Alphaville

The Ripple effect (https://www.ft.com/content/6767d77a-8a7c-3f7d-b1f7-aee777cdb3b8) - FT Alphaville

What does a crypto startup do with $230m? (https://www.ft.com/content/8eeff9c8-9b23-3720-8de6-5a5eb03d413d) - FT Alphaville

What ICO valuations tell us about the state of modern monopolies (https://www.ft.com/content/3216e1e5-ba79-38ee-a543-4b5d71555390) - FT Alphaville

Socialism with trolly characteristics (https://www.ft.com/content/ef1f5c56-aa6b-32be-a5fa-85ced4f0ab85) - FT Alphaville

> Read more articles in **SOMEONE IS WRONG ON THE INTERNET SERIES**

44

Read next:

Alexandra Scaggs

WeWork debt and summer camp